UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/629,947	07/30/2003	Willibald Reitmeier	ZTP01P18003	8887

24131 7590 05/09/2005

LERNER AND GREENBERG, PA
P O BOX 2480
HOLLYWOOD, FL 33022-2480

EXAMINER	
YANG, CLARA I	
ART UNIT	**PAPER NUMBER**
2635	

DATE MAILED: 05/09/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary

Application No. 10/629,947	Applicant(s) REITMEIER, WILLIBALD	
Examiner Clara Yang	Art Unit 2635	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *30 July 2003*.

2a)□ This action is **FINAL**. 2b)☒ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-34* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-14 and 17-34* is/are rejected.

7)☒ Claim(s) *15,16 and 22-28* is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *30 July 2003* is/are: a)☒ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)□ Some * c)□ None of:

1.☒ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date *07/30/03*.

4) □ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) □ Notice of Informal Patent Application (PTO-152)

6) □ Other: _____.

DETAILED ACTION

Information Disclosure Statement

1. The information disclosure statement filed on 30 July 2003 fails to comply with 37 CFR 1.98(a)(2), which requires a legible copy of each cited foreign patent document; each non-patent literature publication or that portion which caused it to be listed; and all other information or that portion which caused it to be listed. It has been placed in the application file, but the information referred to therein has not been considered.

A copy of DE 197 10 546 A1 and its English translation is missing.

2. The information disclosure statement filed on 30 July 2003 fails to comply with 37 CFR 1.98(a)(3) because it does not include a concise explanation of the relevance, as it is presently understood by the individual designated in 37 CFR 1.56(c) most knowledgeable about the content of the information, of each patent listed that is not in the English language. It has been placed in the application file, but the information referred to therein has not been considered.

EPO 910 215 A2 lacks an English translation.

Specification

3. The disclosure is objected to because of the following informalities: On page 7, line 11, change "CCD chip" to "couple charged device (CCD) chip".

Appropriate correction is required.

Allowable Subject Matter

4. Claims 15, 16, and 22-28 are objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

Claim Objections

5. Claim 2 is objected to under 37 CFR 1.75(c), as being of improper dependent form for failing to further limit the subject matter of a previous claim. Applicant is required to cancel the claim(s), or amend the claim(s) to place the claim(s) in proper dependent form, or rewrite the claim(s) in independent form. Claim 2 calls for the step of "assigning the user to one of several authorization levels based upon the biometric recognition of the user", which is broader than the limitation in claim 1 calling for the step of "assigning the user to one of several authorization levels based upon the biometric fingerprint recognition" of the user.

6. Claim 21 is objected to because of the following informalities: Change "CCD chip" to "couple charged device (CCD) chip". Appropriate correction is required.

Claim Rejections - 35 USC § 102

7. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

8. Claims 1-7 and 17-20 are rejected under 35 U.S.C. 102(e) as being anticipated by Tuomela (US 6,792,287).

Referring to claims 1 and 2, Tuomela describes a method for inputting control information into a mobile telephone and states that the method can be incorporated into domestic appliances such as ovens and washing machines (see Col. 6, lines 56-67). Tuomela's method comprises the steps of: (a) fingerprint recognition system 12 performing fingerprint identification/recognition when a user places a finger on sensor plate 10 (see Fig. 2; Col. 3, lines 1-16 and 33-41; and Col. 6, lines 4-7); (b) associating the identified user with a user profile (i.e., assigning the user to one of several user profiles) based on the user's fingerprint (see Col. 5, lines 27-30 and 65-67; and Col. 6, lines 1-4); and (c) enabling a predetermined minimum range of functions of the appliance when fingerprint recognition system 12 fails match the user's fingerprint (see Col. 5, lines 8-12; Col. 6, lines 60-67; and Col. 7, lines 1-8). Because the user profile defines the range of functions a user has access to (see Col. 6, lines 1-7), the user profile indicates a user's authorization level (e.g., greater the range of functions, higher the authorization level).

Regarding claims 3-5, Tuomela's method also includes the step of assigning and storing each user's user profile (see Col. 5, lines 65-67 and Col. 6, lines 1-7), in the appliance, as called for in claim 3. Per Tuomela, the user profile contains personal preferences (i.e., supplementary information) for each registered user and is activated when a user's fingerprint is recognized (see Col. 5, lines 65-67 and Col. 6, lines 1-7), as called for in claims 4 and 5.

Regarding claim 6, as described in the context of using a mobile telephone, Tuomela teaches that personal preferences, which are based on a user's user profile, are activated in lieu of the mobile telephone's default set-up upon recognition of the user's fingerprint (see Col. 5, lines 20-27 and 65-67; and Col. 6, lines 1-7).

Regarding claim 7, Tuomela further suggests the step of parents granting their children minimal user authorization upon recognition of the child's fingerprint (see Col. 5, lines 65-67 and Col. 6, lines 1-7).

Regarding claims 17 and 20, Tuomela discloses that any commercially available fingerprint recognition system can be incorporated and that available fingerprint recognition systems tend to use either capacitive sensors (as called for in claim 17) or optical sensors (as called for in claim 20).

Regarding claims 18 and 19, Tuomela teaches that companies that supply fingerprint recognition systems include Veridicom, Inc. (see Col. 6, lines 47-50). Veridicom, Inc. released the FPS200, which is a silicon capacitive fingerprint sensor (as called for in claim 19), in July 2000. The FPS200 is a silicon chip and has a 256 x 300 semiconductor array (as called for in claim 18).

Claim Rejections - 35 USC § 103

9. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

10. Claims 8-10 are rejected under 35 U.S.C. 103(a) as being unpatentable over Tuomela (US 6,792,287) as applied to claim 7 above, and further in view of Harif (US 2002/0133716).

Regarding claims 8-10, as explained above in the rejection of claim 7, Tuomela teaches the step of parents granting their children minimal user authorization upon recognition of the child's fingerprint (see Col. 5, lines 65-67 and Col. 6, lines 1-7). Though Tuomela discloses that the method and invention can be incorporated in domestic appliances such as ovens (see Col. 6, lines 60-67), Tuomela is silent on the oven having a light and authorizing children to turn on the light as the minimal user authorization, as called for in claim 8. However, the Examiner takes

Official Notice that ovens having a light are well known. Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify Tuomela's method such that a child is granted authorization to turn on the oven's light because authorizing a child to turn on the oven's light enables the child to check the oven's contents without opening the door, thereby protecting the child. Tuomela, however, also fails to teach the step of authorizing a child to activate a temperature of the oven to 50-60° C for reheating prepared foods, as called for in claims 9 and 10.

In an analogous art, Harif teaches an authentication system and method employing rule-based operations for controlling access and operation privileges for vehicles, buildings, homes, computers, equipment, etc. (see Sections [0010]-[0012], [0031], [0034], [0035], [0037], [0038], [0043], [0060]-[0063], and [0069]). Per Harif, when the authentication device is coupled to a stove/oven, the unlocking of the front door with any key other than the parents' keys limits the operation of the stove and range to lower heating temperatures (see Section [0069]). Though Harif is silent on the range of lower heating temperatures, the Examiner takes Official Notice that it is well known that 50-60° C (122-140° F) is a suitable temperature range for reheating prepared foods. Thus, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify Harif's method such that a child is granted authorization to activate a temperature of the stove between 50-60° C because the temperature range is sufficiently high enough to reheat food but low enough to prevent food from burning and potentially causing fires.

Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify Tuomela's method as taught by Harif because reheating prepared food is a relatively safe process and desirable in situations when the child is home alone.

11. Claims 11-14 are rejected under 35 U.S.C. 103(a) as being unpatentable over Tuomela (US 6,792,287) as applied to claim 1 above, and further in view of Anzai (US 6,271,745).

Regarding claim 11-14, Tuomela's method lacks the steps of: (1) protecting the appliance against unintentional changes once an authorized user completes programming the appliance, as called for in claim 11; (2) authorizing changes of the appliance only after the occurrence of a new and subsequent identification of an authorized user, as called for in claim 12; (3) activating a childproofing function of the appliance by placement of a predetermined finger of an authorized user, as required in claim 13; and (4) deactivating the childproofing function of the appliance by reapplication of the predetermined finger of an authorized user, as required in claim 14.

In an analogous art, Anzai teaches a method for inputting control information into a vehicle (see Fig. 1) that comprises: (a) door sensor 11, sensor 13, sensor 15, or sensor 39 sensing a user's fingerprint and providing a signal to central processing unit (CPU) 33 via fingerprint ID and match processor 29, wherein CPU 33 compares the sensed fingerprint to fingerprints stored in non-volatile memory 31 and gives a predetermined level of access if the sensed fingerprint matches to one of the stored user fingerprints (see Col. 3, lines 55-61; Col. 4, lines30-67; and Col. 5, lines 1-28); (b) CPU 33 assigning one of three categories (i.e., authorization levels), such as "owner", "driver", and "non-drive", to a user based on the user's fingerprint (see Col. 4, lines 51-67; Col. 5, lines 1-28; and Col. 7, lines 42-67); and (c) fingerprint ID and match processor 29 enabling an unknown user, such as a valet, to operate the vehicle while preventing access to the glove box or trunk (i.e., predetermined minimum range of operations) (see Col. 8, lines 24-30).

Per Anzai, only an owner is authorized to enroll other individuals, delete individuals, or set up the system, and changes must be made in the menu mode (see Col. 7, lines 5-41), thereby preventing unintentional changes once an owner programs the vehicle and exits the menu mode, as called for in claim 11. In addition, Anzai teaches that a user in the "owner" category (hereinafter referred to as "owner") is able to prevent a non-driver (e.g., a child) from starting the vehicle (see Col. 6, lines 43-48). The processing of enrolling a child to have access to the interior of the vehicle without authorizing the child to operate the vehicle is understood to be childproofing. As shown in Fig. 7, childproofing begins once an owner is verified via door sensor 11 and inside the vehicle at step S31 (see Col. 5, lines 52-62 and Col. 7, lines 5-8). The owner pushes the menu button at step 33, causing the system to confirm that the vehicle is parked at step S35 and to prompt the owner to place a predetermined finger on sensor 39 at step S39 (see Col. 7, lines 10-12). The fingerprint is then scanned, and authorization level of the fingerprint is determined at step S43 (see Col. 7, lines 12-16). Step S43 is a new and subsequent identification of the owner since the owner was previously scanned and identified in order to access the interior of the vehicle; hence Anzai's method includes the step of an owner childproofing the vehicle (i.e., authorizing changes) only after (1) the placement of an owner's predetermined finger on sensor 39, as called for in claim 13, and (2) the occurrence of a new and subsequent identification of the owner, as called for in claims 12. When the child is old enough to drive, the owner can deactivate the childproofing function, as called for in claim 14, by pushing the menu button (see Fig. 7, S33), reapplying a predetermined finger to sensor 39 (see Fig. 7, S39), selecting the option to view/delete an enrolled user (see Fig. 8, S61), deleting the child (see Fig. 10), selecting the option to enroll a user (see Fig. 8, S57), and reenrolling the child as a driver (see Fig. 9, S79 and S85-S97).

Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify Tuomela's method as taught by Anzai because the steps of (1) protecting the appliance against unintentional changes once an authorized user completes programming the appliance, (2) authorizing changes of the appliance only after the occurrence of a new and subsequent identification of user, (3) activating a childproofing function of the appliance by placement of a predetermined finger of an authorized user, and (4) deactivating the childproofing function of the appliance by reapplication of the predetermined finger of an authorized user improve security by enabling a vehicle owner to determine authorized users and their authorization levels, enhance safety by enabling the vehicle owner to childproof the vehicle when necessary, and provide flexibility by enabling the vehicle owner to deactivate the childproofing when the child is old enough to drive (see Anzai, Col. 6, lines 43-48 and 64-67; and Col. 7, lines 15-19).

12. Claim 21 is rejected under 35 U.S.C. 103(a) as being unpatentable over Tuomela (US 6,792,287) as applied to claim 20 above, and further in view of Harkin (US 6,62,8810).

Regarding claim 21, though Tuomela teaches that the fingerprint recognition is performed via an optical sensor (see Col. 6, lines 42-47), Tuomela is silent that the optical sensor performs the optical scanning via a couple charged device (CCD) chip.

In an analogous art, Harkin teaches that conventional optical fingerprint sensing devices require a prism, lenses, a light source, and a CCD chip (see Col. 1, lines 61-63).

Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify Tuomela's optical sensor as taught by Harkin because an optical sensor comprising a CCD chip is conventional and therefore easy to acquire for incorporation into a fingerprint recognition system.

13. Claims 29-34 are rejected under 35 U.S.C. 103(a) as being unpatentable over Tuomela (US 6,792,287) in view of Anzai (US 6,271,745).

Referring to claims 29-31, Tuomela's fingerprint recognition system 12 (i.e., device), as shown in Fig. 2, resides in a household appliance, such as an oven (see Col. 6, lines 60-67), and comprises: (a) image sensor for scanning a fingerprint and providing an analog output, converter 16 for digitizing the analog output, and processor 18 for extracting predetermined features of the fingerprint and providing an output signal (see Col. 3, lines 1-16); (b) processor 20 for receiving the output signal and performing the fingerprint matching process based on the output signal (see Col. 3, lines 33-41); (c) memory 22 connected to processors 18 and 20 for associating/assigning a user profile, which represents a user's authorization level, to the identified user (see Col. 3, lines 26-32; Col. 5, lines 65-67; and Col. 6, lines 1-7); and (d) processor 20 preventing an unknown or identified user from operating the appliance and/or accessing information stored in memory 22 (see Col. 5, lines 8-12 and 65-67; and Col. 6, lines 1-7). Tuomela, however, fails to specifically teach that memory 22 has a hierarchical structure (as called for in claim 29 and in the first limitations of claims 30 and 31) for associating a respective user to one of several user levels (as called for in claim 30) and that processor 20 assigns a respective user to a user level (as called for in claim 31).

In an analogous art, as explained above in the rejection of claims 11-14, Anzai's device, as shown in Fig. 1, comprises: (a) door sensor 11, passenger sensor 13, trunk sensor 15, sensor 39, and fingerprint ID and match processor 29 for reading a user's fingerprint and for supplying an output signal (see Col. 3, lines 55-61 and Col. 4, lines 30-37); (b) control unit 1 having central processing unit (CPU) 33 for receiving processor 29 's output signal and identifying the user based upon the output signal (see Col. 4, lines 37-39); (c) non-volatile memory 31, which is connected to sensors 11, 13, 15, and 39 via CPU 33 and interface unit 35, having a structure for associating an authorized level of access with each stored fingerprint (see Col. 5, lines 21-28); and (d) CPU 33 enabling a predetermined minimum range of functions when the vehicle is operated by a valet (i.e., an unknown user) (see Col. 8, lines 17-33). Because Anzai's CPU 33 is able to identify a user and the user's authorization level based on his/her fingerprint (see Col. 5, lines 21-38; Col. 6, lines 36-48; and Col. 7, lines 42-45), non-volatile memory 31 must have a hierarchical structure for associating an authorized level of access (i.e., user level) with each stored fingerprint, as called for in claims 29 and 30). Per Anzai, a user with an "owner" level of access can assign one of three authorization levels to a respective user via dashboard unit 3 (see Col. 4, lines 40-45; Col. 6, lines 61-67; and Col. 7, lines 1-4 and 42-45); thus CPU 33 assigns a user level to a respective user, as called for in claim 31, based on the enrollment information.

Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify Tuomela's memory 22 as taught by Anzai because a hierarchical structure for storing authorization levels and the range of functions for each authorization level eliminates the need for a user to create a user profile via processor 20 for each authorized user of the oven, thereby making the device easy to use.

Regarding claim 32, Tuomela teaches that in addition to storing a user's authorization level within a user profile, a user's preferences (i.e., supplementary information) are also stored in the user profile (see Col. 5, lines 8-12, 20-34, and 65-67; and Col. 6, lines 1-7).

Regarding claim 33 and 34, Tuomela teaches that processor 20 transmits control information to other devices, such as the mobile telephone's ringer and dialer (see Col. 5, lines 16-27 and Col. 6, lines 1-6), when fingerprint recognition system 12 is incorporated in a mobile telephone. Because processor 20 and the devices are all within the mobile telephone, processor

20 and the device must be connected via a local network. Tuomela discloses that fingerprint recognition system 12 can be incorporated in ovens (see Col. 6, lines 60-67); thus it is understood that processor 20 is connected to other devices within the oven (e.g., the temperature control or the light), as called for in claim 33, via a local network, as called for in claim 34, when fingerprint recognition system 12 is incorporated in an oven.

Conclusion

14. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

- Jean-François Mainguet (2004). *List of fingerprint sensors/sensing area/JFM 2004.* Retrieved 26 April 2005 from http://www.perso.wanadoo.fr/fingerchip/biometrics/types/fingerprint_sensors_list.htm

- Veridicom, *FPS200 Fingerprint* Sensor, 2005.

- Murphy (US 6,225,890) teaches a biometric control system for a vehicle having a memory for storing various authorization levels and associating a registered driver with an authorization level and a processor for assigning an authorization level to each registered driver during the enrollment process. The memory also stores supplementary information for each registered driver.

⌘⌘⌘

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Clara Yang whose telephone number is (571) 272-3062. The examiner can normally be reached on 8:30 AM - 7:00 PM, Monday - Thursday.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Michael Horabik can be reached on (571) 272-3068. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

CY

Clara Yang
Clara Yang